Directory and Security Server for OS/2 Warp

Environment: Today -> Tomorrow

The Information Technology landscape continues to evolve - from mainframes, to personal computers, to client/server local area networks, to three-tier wide area networks. Businesses no longer rely on a single vendor to supply all their IT needs. Virtually every employee in the enterprise is a user of IT technology. The role of IT technology has grown from that of simple bookkeeping and decision support applications, to complex mission critical applications that impact on the entire business. Whereas before a system failure created some irritation and inconvenience, a system failure in todays environment can lead to serious consequences for the business and its customers. So critical is the role of IT in enterprises today, entire enterprises are adopting the attitude of the Chief Information Officer who was focused on the deployment of information technology for strategic and competitive advantage.

Use of Client/Server Applications

Networks and network applications are changing at a fantastic rate Originally, networks did little more that redirect input/output so that end-users could share files and printers. Eventually, applications were developed that exploited the intelligent PCs and Servers that comprised the network - client/server applications. Now we are seeing a new breed of applications that takes this one step further and separates the presentation of information (graphical user interface), from the accessing of the information (resource manager), from the information (data warehouse) - three-tier applications.

These two pie charts show the rapid decline in non-client/server development activity, and the rapid increase in two-tier and three-tier development activity. As always, businesses in transition are the best prospects for new solutions.

Business Problems

Businesses are constantly facing competitive pressures. Some will choose to re-engineer business processes, others will decide to empower their employees. Whatever the response, the Information Technology infrastructure must be flexible enough to adapt quickly and easily. Businesses are evaluating distributed heterogeneous networks for their potential ability to adapt to an uncertain future.

Several inhibitors stand in the way. Multiple hardware and software products from multiple vendors don't always work well together - the end-user becomes the systems integrator. The administration of disparate products from competing companies is difficult. Migration from existing equipment is complex, time consuming and expensive. The end-users must maintain multiple passwords (which can usually be found on a yellow sticky under the telephone or PC keyboard - now that's security!). Networks are susceptible to theft from spoof servers (Trojan Horses), data taps (Sniffer, DatagLANce), etc. Application development is inefficient because the developer must write the application infrastructure from scratch for every application on every platform. And finally, if you want to run a distributed application, then you need to consider a mid-range UNIX/AIX solution, or a mainframe MVS Open Edition solution.

In summary, businesses are reluctant to deploy a distributed heterogeneous network because its perceived to be expensive, complex, and unreliable.

DSS For OS/2 Overview

The remainder of this presentation will focus on what IBM is providing to solve the issues just described.

Directory and Security Server for OS/2 Warp (DSS) extends the LAN Server and Warp Server networks that most businesses are familiar with today by integrating open distributed services. This allows

businesses to connect multiple hardware and software platforms from multiple vendors into a single Cell (a Cell is the basic administrative unit in a distributed environment. It consists of at least one Directory and Security Server). Furthermore, businesses can now run distributed applications across wide area networks using security based on the Kerberos security standard.

The core technology comes from the latest version of the Open Software Foundations (OSF) Distributed Computing Environment (DCE). Customers who are already familiar with the IBM Open Blueprint will notice that DSS provides the Distributed Systems Services layer of the Open Blueprint. Specifically, DSS provides the Directory, Security, Time, Remote Procedure Call (RPC), and Threads services. These services will be covered in more detail shortly.

The packaging is such that customers need only install the Directory Server and Security Server. The other services (Time, RPC, Threads) are integrated into the two servers. The DSS servers can be installed on OS/2 Warp, or Warp plus LAN Server 4, or Warp Server.

Synchronization code is provided for those customers who wish to integrate DSS with LAN Server or Warp Server. The Sync code "glues" the Domain Control database (DCDB) and NET.ACC files on the installed Domain Controller to the DSS Directory Server and Security Server. This allows end-users to continue accessing the network with a single password, and it allows the network administrator to manage the entire network from a single display.

Three DSS Clients for OS/2 are provided to suit various needs. The Administrative Client contains LAN Server and Warp Server Client code, DCE Client code, and an object-oriented, drag and drop, graphical user interface (GUI) for managing the entire network from a single display. The Server Client contains LAN Server and Warp Server Client code, DCE Client code, and the DCE Advertiser Service (more about the Advertiser Service later) is provided for installation on DSS Servers. The Basic DSS Client combines LAN Server and Warp Server Client code and DCE Client code into a single, low-RAM client - perfect for typical end-users, including mobile end-users.

Finally, a Distributed File System (DFS) Client may be installed on any of the above clients. DFS is covered in a later chart. IBM Open Blueprint This graphic shows where DSS fits in the Open Blueprint architecture. Notice how the Distributed Systems Services layer connects the Presentation Services and Application Services (also known as Resource Managers) and Data Base components. DSS provides the foundation for developing, deploying, and maintaining multi-tier distributed applications.

DSS Directory Server

The DSS Directory Server maintains an enterprise-wide directory of information regarding applications, files, databases, and peripherals (printers, modems, etc). It is the single place to go to find or administer resources. Because the Directory was written with large distributed networks in mind, the directory has no architectural limits (unlimited number of users per group, unlimited number of groups per Domain, unlimited number of Domains per Cell, etc). And because the Directory was designed to be platform neutral, it can track and manage resources regardless of platform or vendor.

The Directory may be replicated to provide a level of fault tolerance. To minimize network traffic, only the changes are communicated to the replicas. The directory may also be subsetted and distributed close to the end-users in remote locations to improve their networks performance.

Finally, the Directory contains an Extended Registry Attribute (ERA) function that is helpful in customizing the behavior of a resource or group of resources. For instance, you could use an ERA to limit access to a database to Monday through Friday, 9AM to 5PM.

DSS Security Server

This server is based on Kerberos (three-headed dog that guards the entrance to Hades) technology. It uses a secure third-party authentication server to challenge all clients and all servers that request access to the network. Basically, a user initiates the network signon process by entering a USERID. The Security Server generates a Ticket Granting Ticket that only the real USERID can decrypt. The user machine receives the Ticket Granting Ticket and prompts the user for a password. The password is used to decrypt the Ticket Granting Ticket into a Security Ticket. The Security Ticket is sent to the Application Server to authenticate the user. Application Servers go through a similar process to gain access to the network. Tickets may be set to expire at regular intervals to force clients and servers to re-authenticate themselves periodically. Passwords never travel between clients and servers.

Once a user is authenticated, that user can access any resource in the network, if authorized. authorization is controlled by the Access Control List (ACL) that is associated with the resource.

Encryption is used to protect security tickets and may be used to protect as much of the network traffic as you like - everything from data packet encryption to full user/data privacy. US customers can use encryption based on the Data Encryption Standard (DES). The US government treats DES technology as a national asset and has restricted its export. Non-US customers can use Commercial Data Masking Facility (CDMF) encryption. Basically, DES uses a 56-bit encryption key and CDMF uses a 40-bit key. Both are very difficult to crack (it would take 10 hackers on 10 supercomputers about 10 years), and since the time stamp is contained in the key, the window of opportunity for theft is less than five minutes.

Finally, because this security is based on open industry standards, you can use a single signon to access all DCE compliant networks and resources, even resources that are contained in foreign Cells.

Time Services

One of the classic definitions of a computer is: "A set of processes controlled by a single clock". By providing the wide area network with a common view of time, you are able to treat your WAN as a system.

Time Services works by setting three clocks to an external time source, such as the National Institute of Standards and Technology. Three servers are used to provide for a tie-breaker in the event that two of the servers ever disagree on the exact time. Time services are very important when working with databases or posting transactions. Everyone understands the importance of ensuring that debits and credits and database updates are posted in the correct sequence.

Also, when problems occur in a large network, there tends to be a cascade or domino effect. A "drive full" condition will cause an application to fail, which will cause several users to get errors, which will cause the network administrators phone to light up. Now the administrator can look at the time-stamps to establish the sequence of events, and therefore the cause and effects of the problems.

DSS Remote Procedure Call

The Remote Procedure Call (RPC) is a programming model that, most simply stated, extends the familiar Call/Return programming model. The RPC Call is capable of calling a subroutine on a remote system, and then returning the information to the calling system.

Because the RPC is based on open standards, the calling and called systems can be on disparate platforms from different vendors. Interoperability is virtually guaranteed because the core code is based on much more than just a paper specification, it's based on actual code that's provided by OSF to IBM and every other OSF member.

The RPC is a platform and vendor independent programming model that allows applications to run in heterogeneous environments.

Furthermore, RPC shields application developers from concerns about data representation (ASCII vs EBCDIC), platform architectures (e. g. Big Endian for MVS vs Little Endian for PC) and communication layers. The benefit of this is that applications can now be quickly and easily ported to other platforms, regardless of hardware architecture or communication implementation.

The DSS clients provide the RPC interface that enables distributed application support on heterogeneous platforms. All DSS clients are fully OSF DCE V1.1 compatible.

Distributed File System

The Distributed File System (DFS) is an application that runs on DSS clients. It give the end-user the illusion that the entire contents of multiple DFS servers (such as AIX DFS and/or MVS DFS servers) are available as local resources. Performance techniques such as client-side caching are employed to ensure good response time regardless of location of the various DFS servers.

DSS Value

This foil and the following foil are summaries that recap several of the key benefits that we have already discussed.

DSS provides a security mechanism that was specifically designed to protect wide area networks. It authenticates clients and servers, allows end-users to access only those resources that they are specifically authorized to use, and it provides an encryption algorithm that is so robust, the US government restricts it from export. DSS provides non-US customers with the Commercial Data Masking Facility for encryption.

DSS provides a distributed application framework for developers. Since the directory and security middleware is supplied by DSS, developers can focus on writing the application's business logic instead of the application's infrastructure. Since the infrastructure is built on open industry standards, applications can be easily ported to disparate platforms. Finally, by using OSF supplied code for the infrastructure, developers have fewer new lines of code to create, which means fewer chances for errors, which means reduced maintenance time and expense.

Information technology architectures are typically brittle and hard to change. We all know, based on past experience, that the future is unpredictable. We also know that we need to be responsive to changes in our environment - whether those changes are caused by our competition, technology, legislation, etc. Finally, we need to be able to quickly organize to take advantage of new opportunities. Competitive advantages disappear all too quickly when business are unable to exploit them.

DSS provides a scalable architecture that supports an unlimited number of users per group, unlimited groups per domain, unlimited number of domains per cell, etc. DSS operates across multiple platforms from multiple vendors. It even allows end-users to access resources in foreign cells.

IBM Value - DCE Made Easy

Some people would almost consider this an oxymoron. "DCE" and "easy" are two words that seldom appear in the same sentence. This is one of the key elements that differentiates IBM's offering from that of other DCE vendors.

Right from the start, DSS is designed to be installed and configured with maximum ease. If you already have Warp Server installed, you can launch the DSS installation process from the "Install" icon. The DSS installation automatically discovers the location of any DCE servers that are already installed - no need to look-up or key-in any IP addresses.

You install DSS on servers and clients at your own pace (more about this in the following two foils). User IDs and resource names are preserved during installation (unlike migration programs from other vendors that can delete duplicate names). For instance: DSS gives you the opportunity to tag identical USERIDs as duplicates that should be combined, or as duplicates that should be renamed so that they can retain their unique characteristics.

Users will benefit from the simplicity and convenience of having a single signon to access all their LAN Server, Warp Server, and DCE services. Now users can easily access any resource on any platform from any vendor, anywhere. Best of all, there is virtually nothing new for end-users or administrators to learn.

DSS simply extends the same award-winning interface that users and administrators are using today.

Application developers will benefit from having a proven application services infrastructure provided. Since it's based on open standards, source code can be easily ported to other platforms. A Managed Objects Class Library (MOCL) is provided to simplify the writing of complex and/or repetitive administrative tasks. And to help programmers get started with DSS, samples are provided that demonstrate features and functions of distributed applications.

Administrators now have a single logical view of all users and resources on the local-area or wide-area network. Management is performed from a single piece of glass using the award-winning drag and drop graphical user interface. If you can point and click, you can manage a network. The DSS interface is a logical and intuitive extension to the LAN Server and Warp Server interface that administrators are using today.

Finally, DSS is based on the latest code available from the OSF. IBM, along with over 300 other OSF members, receives a tape from the OSF that contains the base services (directory, security, time, RPC, and threads) for a distributed computing environment. It's this agreement on standards that allows the computer industry to support, and customers to enjoy, truly open distributed heterogeneous client/server computing.

Resource Domains - Migration Made Easy

Customer who already have LAN Server or Warp Server domains installed will appreciate the ease with which they can consolidate those domains into a single DSS cell. All that's required is a Directory Server installation, a Security Server installation, and Synchronization code installations on each domain controller. Domain administrators can continue to manage resources in their individual domains (now known as Resource Domains) as they had before, or the DSS administrator can now manage all users and resources across all domains as a single cell. End-users can now access any resource anywhere in the cell - if authorized.

Directory and Security Server

Rollout Options: 2 Domains -> 1 Cell

This foil outlines an example of a phased rollout of DSS, and describes the benefits that accumulate to the company at each phase of the rollout.

Phase I: Install DSS Synchronization code on the Domain Controllers and you can consolidate multiple domains into a single cell. End-users can now access any resource in the cell (where they could previously only access resources in their domain), and administrators can administer all users and resources from a single display.

The Synchronization code synchronizes the LAN Server and Warp Server DCDB and NET.ACC databases with the DSS Directory and Security servers. End-users continue to logon to LAN Server and

Warp Server as they always have, but USERIDs and passwords are now located in a registry that acts as a single repository for all authentication information.

Phase II: Install DSS on Additional Servers, and now all your servers can use the third-party authentication security service provided in DSS. Once all the Additional Servers are updated, the DCDB and NET.ACC databases need no longer be synchronized with the Directory and Security servers. The LAN Server and Warp Server architecture is replaced with the DSS architecture. The DSS architecture allows for an unlimited number of users in a group, an unlimited number of groups in a domain, and an unlimited number of domains in a cell.

Phase III: Install DSS on all client workstations, and now all your clients can access resources that reside in foreign cells. Clients can now use the third-party authentication service, and clients can now run RPC applications.

Enterprise C/S Issues

This foil is an introduction to the following five foils that describe how DSS can solve fundamental, yet difficult, challenges that companies face as they deploy client/server applications. The remainder of this foil is self-explanatory.

Availability

In this example, a Payroll service is installed on two servers in a network. Clients never actually request a specific server in a DSS or DCE network . Clients request the desired service and let the Directory Service route the request to server that contains the service. If one of the Payroll servers goes down, clients will automatically connect to the other Payroll server.

Performance

Adding additional servers to increase capacity across an overloaded network is usually a long and complicated task. In a DSS or DCE network, the Advertiser Service alerts the Directory that a service is available. The Directory Server uses a "workload fairness algorithm" to assign clients to the least utilized servers in the network. Workload balancing is handled automatically as clients signon and access services in the network.

Integrity

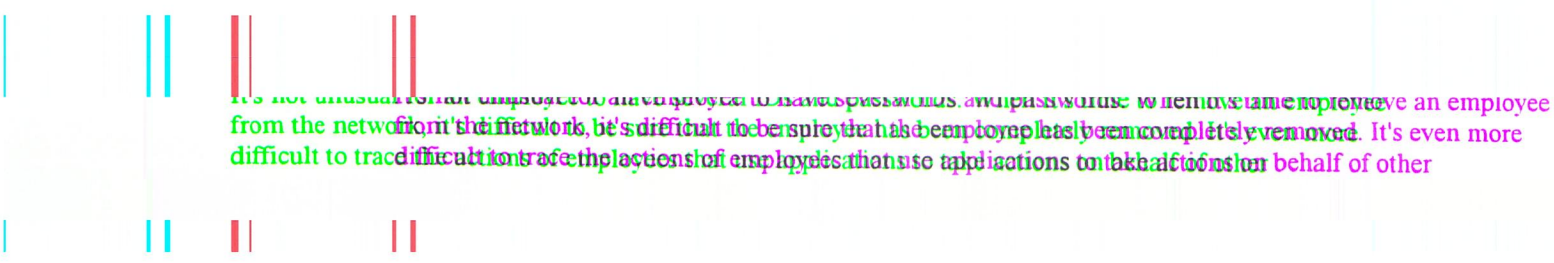
Many networks run the risk of having transactions intercepted or recorded, altered, and then played-back into their data repository. In the case of financial transactions, the results can be disastrous. DSS allows you to select the level of security/encryption that's right for you. In this example, just encrypting the checksum character for the data packet would be sufficient to protect data integrity.

Change Control

Changes to servers and clients can be introduced gradually and automatically by using Access Control Lists to control which clients access which servers. For instance: you could specify that clients should only access those servers that are at the same code level or later as that of the client. That way, as clients are upgraded, they will automatically start using the upgraded servers.

ecurity

Security



applications. DSS and DCE solve both these problems. First, a single repository is provided for all USERIDs and passwords. This allows administrators to simply remove a USERID from the system with a single command. Second, DSS and DCE have an audit facility that can track user requests, and can even track requests that resulted from credential forwarding.

Competition

DSS provides an enterprise-wide directory service that Microsoft can't match, and application server capabilities that Novell can't match.

Competitive Solutions

Novell NetWare 4.1 contains NetWare Directory Services (NDS) that Novell markets as an enterprise-wide directory. NDS only works within a single NDS directory - clients can't access resources in "foreign" NDS cells.

Microsoft NT Server 3.5.1 contains Trusted Domains which Microsoft has started marketing as an enterprise directory.

Trusted Domains are couplets that can be managed as a single domain once you set up all of the required trust relationships. Two domains require two relationships, three domains require six relationships, four domains require twelve relationships,.. This is an architecture that does not scale.

Competition - NT Server

Microsoft is leveraging it's success in desktop products. They claim that the best company for servers is the company that provides the clients. Microsoft will also present their solutions as secure since they achieved C2 certification in '95. The application server capabilities of NT Server combined with the broad ISV support has allowed Microsoft to start capturing market share from Novell.

Things you should know:

Microsoft claims to have an enterprise directory - they don't. They have a domain directory - just like LAN Manager, LAN Server, and Warp Server. Without changing a line of code, Microsoft is now claiming their domain directory is an enterprise-wide directory, while at the same time claiming that they will ship an enterprise directory when they ship Cairo (which even by Microsoft estimates is in 1997). By the way, Microsoft doesn't even support aliases - something IBM has offered since LAN Server.

Regarding security: If your network is not secure and you run your business accordingly - that' s OK. If your network is secure and you run your business accordingly - that's OK. If you falsely believe your network is secure and you run your business accordingly - that's trouble.

Microsoft achieved the standalone version of C2 certification in 1995, and it's limited to 3 very specific hardware models. None of the certified configurations contained any adapter cards. In other words, there's no way to connect any of the certified configurations to a network without violating the certification. Furthermore, NT Server doesn't contain any encryption or third-party authentication capabilities.

Microsoft claims to support DCE, but they don't offer any Directory or Security servers, and the Remote Procedure Call that they supply is an emulated incompatible subset (79 out of 97 APIs) of the Open Software Foundation API set. Microsoft is relying on DEC and Gradient to deliver DCE support for Microsoft products, but neither company is offering DFS support for Microsoft products. And neither company has integrated their DCE support with NT Server to the degree that IBM has integrated DCE support with LAN Server and Warp Server.

Competition - NetWare 4.1

Novell has dominated the file and print serving market for years. As networking requirements shift from simple redirected I/O to more complex application serving and multi-tier distributed computing, Novell has been unable to respond (abandoned AppWare, abandoned UnixWare, abandoned UNIX System Labs), and their market share declined in 1995.

The Novell NDS structure has problems right from the installation. Duplicate names from NetWare 2.x and 3.x networks are deleted when you attempt to add them to the new NDS network. NDS doesn't just act like it's the center of the universe, it acts like it's the entire universe. Users can't access resources in other NDS networks, and it's very difficult to consolidate two NDS networks into a single NDS network. Novell achieved the network version of C2 certification in 1995. Novell's certification requires an $800 device to be attached to every node in the network. And it's still not third-party authentication.

Novell doesn't offer any DCE products and their API set is proprietary. Novell and HP did publish a joint press release in 3Q95 where they committed to "integrate" NDS with DCE. Details are still unavailable.

Complete Family of Warp Networking Products

IBM is committed to networking offers a complete selection of networking products that support open, standards-based, computing.

Solutions for Multiple Markets

DSS provides different benefits to different market segments:

Large businesses and institutions will benefit from the simplified administration from consolidating multiple domains into a single cell. End-users will benefit from being able to do things across wide-area networks as easily as they can do things on a local-area network today. Furthermore, DSS uses a proven technology (Kerberos) to provide enterprise-wide security.

Medium businesses and departmental workgroups will benefit from the standards-based Remote Procedure Call that hides differences in data representation and isolates applications from the communications layer. This allows disparate machines and databases to be easily networked together. And it allows applications to be easily ported from one platform to another.

Small businesses will benefit from the ability to run secure distributed applications on industry standard hardware. Companies no longer need to buy mid-range or mainframe computers to run secure, distributed applications.

DCE Resources

IBM has a comprehensive infrastructure in place to encourage and support the development, deployment, and maintenance of secure multi-tier distributed applications in heterogeneous environments.